UNITED STATES DISTRICT COURT

for the

Middle District of North Carolina

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

2019 Toyota Camry assigned North Carolina license plate B124CP

Case No. 1:24MJ124

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment C hereto and incorporated herein by reference

located in the Middle District of North Carolina, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment D hereto and incorporated herein by reference

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2252A(a)(2)(A)	Receiving or Distributing Child Pornography
18 U.S.C. § 2252A(a)(5)(B)	Possessing or Accessing with Intent to View Child Pornography

The application is based on these facts:

See attached affidavit which is attached hereto and incorporated herein by reference

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/S/William Thompson
Applicant's signature

William D. Thompson, SA, HSI
Printed name and title

UPA

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone after email identity *(specify reliable electronic means)*.

Date: 04/05/24

Judge's signature

City and state: Greensboro, North Carolina

L. Patrick Auld, United States Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, William D. Thompson, a Special Agent ("SA") with Homeland Security Investigations ("HSI"), being duly sworn, depose and state as follows:

INTRODUCTION

1. I am investigating offenses related to child sexual exploitation. This Affidavit is submitted in support of applications under Rule 41 of the Federal Rules of Criminal Procedure for warrants to search the premises located at 100 Village Circle Way, Apartment 532, Durham, North Carolina 27713 (the "SUBJECT PREMISES"), more specifically described in Attachment A, Alec Joseph WHITE's person, more specifically described in Attachment B, and a 2019 Toyota Camry, registered to Alec Joseph WHITE and assigned North Carolina license plate number B124CP (the "SUBJECT VEHICLE'), more specifically described in Attachment C, for contraband and evidence, fruits, and instrumentalities of violations of Title 18 U.S.C. §§ 2252A(a)(2)(A) and 2252A(a)(5)(B), which items are more specifically described in Attachment D.

2. The statements in this Affidavit are based in part on information provided by other law enforcement officers and on my investigation of this matter. Since this Affidavit is being submitted for the limited purpose of

securing a search warrant, I have not included each, and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of Title 18 U.S.C. §§ 2252A(a)(2)(A) and 2252A(a)(5)(B) are presently located at the SUBJECT PREMISES, on the person of Alec Joseph WHITE, and in the SUBJECT VEHICLE.

AFFIANT BACKGROUND

3. I am a SA of the U.S. Department of Homeland Security ("DHS"), HSI, formerly the United States Customs Service ("USCS"), having been so employed since December 2001, and I am currently assigned to the HSI Raleigh office in Cary, North Carolina. While employed by HSI, I have investigated federal criminal violations related to high technology and cybercrime, child exploitation, child pornography, and child molestation. I have received training from the Federal Law Enforcement Training Center ("FLETC") and other law enforcement agencies in the areas of child exploitation and pornography investigations and pedophile behavior. As part of my current duties, I investigate criminal violations relating to child exploitation and child pornography, including violations pertaining to the illegal production, distribution, receipt, and possession of child pornography. I

have had the opportunity to observe and review numerous examples of child pornography as defined in 18 U.S.C. § 2256 in various forms of media, including computer media. In addition, I have participated in the execution of numerous search warrants involving child exploitation, child pornography, and child molestation offenses and I am in routine contact with experts in the fields of computers, computer forensics and Internet investigations.

4. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2251, 2252, and 2252A, and I am authorized by law to request a search warrant.

STATUTORY AUTHORITY

5. As noted above, this investigation concerns alleged violations of the following:

a. 18 U.S.C. § 2252A(a)(2)(A) prohibits a person from knowingly receiving or distributing child pornography, as defined in 18 U.S.C. § 2256(8), using any means and facility of interstate and foreign commerce, that has been mailed, or that has been shipped and transported in and affecting interstate and foreign commerce by any means, including by computer. Attempts and conspiracies are also violations of this statute. 18 U.S.C. § 2252A(b)(1).

b. 18 U.S.C. § 2252A(a)(5)(B) prohibits a person from knowingly possessing or knowingly accessing with intent to view any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer. Attempts and conspiracies are also violations of this statute. 18 U.S.C. § 2252A(b)(2).

DEFINITIONS

6. The following definitions apply to this Affidavit and Attachment:

a. "Chat," as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

b. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but

that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

c. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. Child Sex Abuse Material or "CSAM" has the same meaning.

d. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high-speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, other mobile phones, and other mobile devices.

e. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, "thumb," "jump," or "flash" drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

f. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security

software or code may also encrypt, compress, hide, or "booby- trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

g. The "dark web," is a portion of the "deep web[1]" of the Internet, where individuals must use an anonymizing software or application called a "darknet" to access content and websites. Within the dark web, criminal marketplaces operate, allowing individuals to buy and sell illegal items, such as drugs, firearms, and other hazardous materials, with greater anonymity than is possible on the traditional Internet (sometimes called the "clear web" or simply the "web"). These online market websites use a variety of technologies, including the Tor network (defined below) and other encryption technologies, to ensure that communications and transactions are shielded from interception and monitoring. Famous dark web marketplaces, also called Hidden Services, such as Silk Road, AlphaBay, and Hansa (all of which have since been shut down by law enforcement), operated similarly to clear web commercial websites such as Amazon and eBay, but offered illicit goods and services.

[1] The deep web is the portion of the Internet not indexed by search engines. Examples are databases and internal networks belonging to private industry, government agencies, or academic institutions.

h. The "Domain Name System" or "DNS" is a system that translates readable Internet domain names such as www.justice.gov into the numerical Internet protocol addresses of the computer server that hosts the website.

i. "Geolocated," as used herein, refers to the identification of the geographical location of (a person or device) by means of digital information processed via the Internet.

j. A "hash value" is a unique multi-character number that is associated with a computer file. Some computer scientists compare a hash value to an electronic fingerprint in that each file has a unique hash value. Any identical copy of the file will have exactly the same hash value as the original, but any alteration of the file, including even a change of one or two pixels, would result in a different hash value. Hash values represent large amounts of data as much smaller numeric values, so they are used with digital signatures.

k. A "hidden service," also known as an "onion service," is a website or other web service that is accessible only to users operating within the Tor anonymity network.

l. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and

businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

m. An "Internet protocol address" or "IP address," (IP) as used herein, refers to a unique numeric or alphanumeric string used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most ISPs control a range of IP addresses. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

n. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

o. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

p. "Mobile application" or "chat application," as used herein, are small, specialized programs downloaded onto mobile devices, computers and other digital devices that enable users to perform a variety of functions, including engaging in online chat and sending or receiving images and videos.

q. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

r. "Remote computing service", as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

s. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person.

t. A "storage medium" is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, "thumb," "jump," or "flash" drives, CD-ROMs, and other magnetic or optical media.

u. The "Tor network," or simply "Tor" (an abbreviation for "The Onion Router"), is a special network of computers on the Internet, distributed around the world, designed to conceal the true IP addresses of the computers accessing the network, and, thereby, the locations and identities of the network's users. Tor also enables websites to operate on the network in a way that conceals the true IP addresses of the computer servers hosting the websites, which are referred to as "hidden services" on the Tor network. Such hidden services operating on Tor have complex web addresses, generated by a computer algorithm, ending in ".onion" and can only be accessed through specific web browser software, including a browser known as "Tor Browser," designed to access the Tor network. Examples of hidden services websites are the previously cited AlphaBay and Hansa. Tor is available on cellphones using the Android and Apple operating systems by installing an application that puts a TOR-enabled internet browser on a user's cellphone, which then routes the phone's IP address through different servers all over the world, making it extremely difficult to track.

v. "URL" is an abbreviation for Uniform Resource Locator and is another name for a web address. URLs are made of letters, numbers, and other symbols in a standard form. People use them on computers by clicking a pre-prepared link or typing or copying and pasting one into a web browser to make the computer fetch and show some specific resource (usually a webpage) from another computer (web server) on the Internet.

w. "Vendors" are the dark web's sellers of goods and services, often of an illicit nature, and they do so through the creation and operation of "vendor accounts" on dark web marketplaces. Customers, meanwhile, operate "customer accounts." Vendor and customer accounts are not identified by numbers, but rather monikers or "handles," much like the username one would use on a clear website. If a moniker on a particular marketplace has not already been registered by another user, vendors and customers can use the same moniker across multiple marketplaces, and based on seller and customer reviews, can become well known as "trusted" vendors or customers. It is also possible for the same person to operate multiple customer accounts and multiple vendor accounts at the same time. For example, based on my training and experience, I know that one person could have a vendor account that he or she uses to sell illegal goods on a dark web marketplace in exchange for cryptocurrency; that same vendor could also have a different customer account

that he or she uses to exchange cryptocurrency earned from vendor sales for fiat currency.[2] Because they are separate accounts, a person could use different accounts to send and receive the same cryptocurrency on the dark web. I know from training and experience that one of the reasons dark web vendors have multiple monikers for different vendor and customer accounts, is to prevent law enforcement from identifying which accounts belong to the same person, and who the actual person is that owns or uses the accounts.

x. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether, or not stored in a permanent format.

y. A "website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

CRYPTOCURRENCY (BITCOIN)

[2] Fiat currency is currency issued and regulated by a government such as the U.S. Dollar, Euro, or Japanese Yen.

7. "Cryptocurrency," a type of virtual currency, is a decentralized, peer-to peer, network-based medium of value or exchange that may be used as a substitute for fiat currency to buy goods or services or exchanged for fiat currency or other cryptocurrencies. Examples of cryptocurrency are Bitcoin, Litecoin, and Ether. Cryptocurrency can exist digitally on the Internet, in an electronic storage device, or in cloud-based servers. Although not usually stored in any physical form, public and private keys (described below) used to transfer cryptocurrency from one person or place to another can be printed or written on a piece of paper or other tangible object. Cryptocurrency can be exchanged directly person to person, through a cryptocurrency exchange, or through other intermediaries. Generally, cryptocurrency is not issued by any government, bank, or company; it is instead generated and controlled through computer software operating on a decentralized peer-to-peer network. Most cryptocurrencies have a "blockchain," which is a distributed public ledger, run by the decentralized network, containing an immutable and historical record of every transaction.[3] Cryptocurrency is not illegal in the United States.

[3] Some cryptocurrencies operate on blockchains that are not public and operate in such a way to obfuscate transactions, making it difficult to trace or attribute transactions.

8. Bitcoin[4] ("BTC") is a type of cryptocurrency. Payments or transfers of value made with bitcoin are recorded in the Bitcoin blockchain and thus are not maintained by any single administrator or entity. As mentioned above, individuals can acquire bitcoin through exchanges (i.e., online companies which allow individuals to purchase or sell cryptocurrencies in exchange for fiat currencies or other cryptocurrencies), bitcoin ATMs, or directly from other people. Individuals can also acquire cryptocurrencies by "mining." An individual can "mine" bitcoins by using his or her computing power to solve a complicated algorithm and verify and record payments on the blockchain. Individuals are rewarded for this task by receiving newly created units of a cryptocurrency. Individuals can send and receive cryptocurrencies online using many types of electronic devices, including laptop computers and smart phones. Even though the public addresses of those engaging in cryptocurrency transactions are recorded on a blockchain, the identities of the individuals or entities behind the public addresses are not recorded on these public ledgers. If, however, an individual or entity is linked to a public address, it may be possible to determine what transactions were conducted by that individual or

[4] Since Bitcoin is both a cryptocurrency and a protocol, capitalization differs. Accepted practice is to use "Bitcoin" (singular with an uppercase letter B) to label the protocol, software, and community, and "bitcoin" (with a lowercase letter b) to label units of the cryptocurrency. That practice is adopted here.

entity. Bitcoin transactions are therefore sometimes described as "pseudonymous," meaning that they are partially anonymous. And while it's not completely anonymous, bitcoin allows users to transfer funds more anonymously than would be possible through traditional banking and financial systems.

9. Cryptocurrency is stored in a virtual account called a "wallet." Wallets are software programs that interface with blockchains and generate and/or store public and private keys used to send and receive cryptocurrency. A public key or address is akin to a bank account number, and a private key is akin to a PIN number or password that allows a user the ability to access and transfer value associated with the public address or key. To conduct transactions on a blockchain, an individual must use the public address (or "public key") and the private address (or "private key"). A public address is represented as a case-sensitive string of letters and numbers, 26–25 characters long. Each public address is controlled and/or accessed through the use of a unique corresponding private key, the cryptographic equivalent of a password or PIN, needed to access the address. Only the holder of an address' private key can authorize any transfers of cryptocurrency from that address to another cryptocurrency address.

10. Although cryptocurrencies such as bitcoin have legitimate uses, cryptocurrency is also used by individuals and organizations for criminal purposes such as money laundering and is an oft used means of payment for illegal goods and services on hidden services websites operating on the Tor network. By maintaining multiple wallets, those who use cryptocurrency for illicit purposes can attempt to thwart law enforcement's efforts to track purchases within the dark web marketplaces.

11. Exchangers and users of cryptocurrencies store and transact their cryptocurrency in a number of ways, as wallet software can be housed in a variety of forms, including on a tangible, external device ("hardware wallet"), downloaded on a PC or laptop ("desktop wallet"), with an Internet-based cloud storage provider ("online wallet"), as a mobile application on a smartphone or tablet ("mobile wallet"), printed public and private keys ("paper wallet"), and as an online account associated with a cryptocurrency exchange. Because these desktop, mobile, and online wallets are electronic in nature, they are located on mobile devices (e.g., smart phones or tablets) or at websites that users can access via a computer, smart phone, or any device that can search the Internet. Moreover, hardware wallets are located on some type of external or removable media device, such as a USB thumb drive or other commercially available device designed to store cryptocurrency (e.g. Trezor, Keepkey, or Nano Ledger).

In addition, paper wallets contain an address and a QR code[5] with the public and private key embedded in the code. Paper wallet keys are not stored digitally. Wallets can also be backed up into, for example, paper printouts, USB drives, or CDs, and accessed through a "recovery seed" (random words strung together in a phrase) or a complex password. Additional security safeguards for cryptocurrency wallets can include two-factor authorization (such as a password and a phrase). I also know that individuals possessing cryptocurrencies often have safeguards in place to ensure that their cryptocurrencies become further secured in the event their assets become potentially vulnerable to seizure and/or unauthorized transfer.

12. To transfer BTC to another BTC address, the sender transmits a transaction announcement, which is cryptographically signed with the sender's private key, across the peer-to-peer BTC network. To complete a transaction, a sender needs only the BTC address of the receiving party (who also has a private key) and the sender's own private key. These two keys by themselves rarely reflect any identifying information about either sender or recipient. As a result, little-to-no personally identifiable information about the sender or recipient is transmitted in a BTC transaction itself. Once the sender's

[5] A QR code is a matrix barcode that is a machine-readable optical label.

transaction announcement is verified by the network, the transaction is added to the blockchain.

13. While a BTC address owner's identity is generally anonymous (unless the owner opts to make information about the owner's BTC address publicly available), investigators can use the blockchain to identify the owner of a particular BTC address. Because the blockchain serves as a searchable public ledger of every BTC transaction, investigators can trace transactions to, and among other recipients, BTC exchangers. Because BTC exchangers generally collect identifying information about their customers, as discussed below, subpoenas or other appropriate legal process submitted to exchangers can, in some instances, reveal the true identity of an individual responsible for a BTC transaction.

14. Blockchain analysis can also, in some instances, reveal whether multiple BTC addresses are controlled by the same individual or entity. For example, the proprietor of a website that accepts payment via BTC may create multiple different BTC addresses to receive payments from different customers. If the proprietor later decides to consolidate the BTC that it has received from those customers, the proprietor may group those BTC addresses together to send a single transaction into one BTC account. Each of those many BTC addresses would then appear as "inputs" on a single transaction on the

blockchain. Therefore, if a known BTC address appears as an "input" on a single transaction alongside other unknown addresses, this may indicate that these addresses are all controlled by the same user. Additional examination of these BTC addresses and their activity on the blockchain may also reveal further information about the user and his/her previous transactions.

15. Law enforcement uses sophisticated commercial services offered by several different blockchain-analysis companies to investigate bitcoin transactions in this fashion. These companies analyze the blockchain to identify individuals or groups involved with bitcoin transactions. Specifically, by analyzing the data underlying bitcoin transactions, these companies create large databases that group bitcoin transactions into "clusters." This third-party analysis allows law enforcement to identify BTC addresses that are included as "inputs" in the same transaction, as described above, and "cluster" these addresses together. After using this type of data in numerous unrelated investigations, law enforcement has found the clustering information and analysis provided by these companies to be reliable.

16. Banks and law enforcement organizations worldwide use this third-party blockchain-analysis software as, among other things, an anti-money laundering tool. It has supported many investigations and been the basis for numerous search and seizure warrants. Further, computer scientists

have independently shown that they can use these "clustering" methods as clues to analyze how BTC are aggregated or split up, and to identify BTC addresses and their respective account owners.

17. As described herein, based on investigation to date, various Tor .onion sites appear to assign each user accessing the site a unique BTC address to which the user can send funds for purchasing account privileges. Based on prior investigations, law enforcement is aware that creating a payment system in which purchasers send payments to unique addresses associated with a centralized operator allows blockchain-analysis software to identify which payments are going into a cluster of BTC addresses associated with the recipient of the payments.

18. One of the functions of the third party who operates clustering analysis software is to proactively seek out sites on the Tor network, and related BTC clusters, that may be engaged in illicit activity, in part to allow institutions that are required to perform due diligence to ensure they are not sending funds to illicit sites.

DARKNET

19. The Darknet is a network of computers that offer restricted access that is used mainly for peer-to-peer transactions, including payment transactions. Darknet markets commonly sell illicit goods such as drugs, stolen

information, weapons, and child pornography. The transactions in Darknet markets are anonymized and typically use cryptocurrency like Bitcoin and other virtual currencies to protect the identity of the seller and buyer.

TOR

20. Tor is a computer network designed to facilitate anonymous communication over the Internet. The Tor network does this by routing a user's communications through a globally distributed network of relay computers, or proxies, rendering conventional IP address-based methods of identifying users ineffective. To access the Tor network, a user must install Tor software either by downloading an add-on to the user's web browser or by downloading the free "Tor browser bundle," which is available at www.torproject.org.[6] When a Tor user accesses a website, only the IP address of the last relay computer (the "exit node"), as opposed to the user's actual IP address, appears on the website's IP address log. Currently, there is no practical method to trace a user's actual IP address back through those Tor relay computers.

21. The Tor Network also makes it possible for users to operate websites, called "hidden services," in a manner that conceals the true IP address of the computer hosting the website. Like other websites, "hidden

[6] Additional information outlining Tor and how it works is publicly accessible at www.torproject.org.

services" are hosted on computer servers that communicate through IP addresses. However, hidden services have unique technical features that conceal the computer server's location. Unlike standard Internet websites, a Tor-based web address is comprised of a series of 16 algorithm-generated characters, for example "asdlk8fs9dflku7f," followed by the suffix ".onion." Ordinarily, investigators can determine the IP address of the computer server hosting a website by simply looking it up on a publicly available Domain Name System ("DNS") listing. Unlike ordinary internet websites, however, there is no publicly available DNS listing through which one can query the IP address of a computer server that hosts a Tor hidden service. So, while law enforcement agents can view and access hidden services that are facilitating illegal activity, they cannot determine the IP address of a Tor hidden service via public lookups. Additionally, as with all Tor communications, communications between users' computers and a Tor hidden-service web server are routed through a series of intermediary computers. Accordingly, neither law enforcement nor hidden-service users can use public lookups or ordinary investigative means to determine the true IP address, and therefore the location of a computer server that hosts a hidden service.

COINBASE

22. Coinbase is a cryptocurrency provider. On its website, it describes its services as "a secure online platform for buying, selling, transferring, and storing cryptocurrency." (See Coinbase.com).

23. As defined on Coinbase's website, TXHASH "is a unique identifier, similar to a receipt, that serves as proof that a transaction was validated and added to the blockchain."

24. Coinbase is legally required to gather Know Your Customer ("KYC") data and verify the identity of its users. KYC data includes the subscriber/user's name, date of birth, street address, and last four digits of their social security number. The subscriber/user is also required to submit a valid government-issued photo identification, such as a driver's license.

INTERNET WATCH FOUNDATION

25. Information relied upon in this affidavit was obtained from the Internet Watch Foundation ("IWF"). IWF is an independent, non-profit charitable organization based in the United Kingdom that identifies those who distribute/trade child sexual abuse material ("CSAM") online. I have reviewed their website, which states, the IWF:

> works in partnership with the internet and tech industries, global law enforcement, governments, the education sector, charities and non-profits across the world and the public to minimise, disrupt and stop the availability of child sexual abuse images and videos

hosted anywhere in the world, and non-photographic child sexual abuse images hosted in the UK.

26. The IWF is separate from government and law enforcement in the United Kingdom and operates as a charity. However, they work in partnership with law enforcement to identify those who trade images and videos of child sex abuse online.

27. Based on my training, experience, and research, IWF is a trusted organization whose independent investigation and information has been relied upon by law enforcement around the world including in the United States. They operate akin to, and collaborate with, the National Center for Missing and Exploited Children ("NCMEC"), who act in a similar capacity in the United States.

28. IWF investigates complaints received from the public or through Internet service providers and others. When IWF initiates an investigation, they document their findings in an IWF report.

PROBABLE CAUSE

29. On or about September 7, 2023, HSI Miami received information from Coinbase indicating Alec WHITE's Coinbase account, User ID 5e94b88a25792c1aafb31eb9, appeared to have been utilized to send BTC on

the Darknet to a Tor .onion[7] website(s) containing CSAM and advertising the ability to purchase access to additional CSAM. Subsequent database queries by HSI Miami revealed Alec WHITE's most recent probable residence was in the Middle District of North Carolina (MDNC), prompting an investigative referral to HSI Raleigh.

30. On or about September 13, 2023, I received the investigative referral and two (2) associated Coinbase reports from HSI Miami. On this date, I reviewed the Coinbase reports revealing they provided the web address for a Tor .onion website, hereafter referred to as **Tor CSAM site 1**. Coinbase documented **Tor CSAM site 1** appeared to host child pornography and contained instructions on how to purchase "premium access" to the site. Coinbase further documented **Tor CSAM site 1** directed purchasers to deposit 0.0006654 BTC to BTC address bc1qsstk2j9p7eklzmeq2h3zegdj6ua5vacu2r7yq7, hereafter referred to as **Tor CSAM site 1 BTC address**.

31. Coinbase also reported they identified, through the utilization of Darknet and financial analysis tools, that the **Tor CSAM site 1 BTC**

[7] As outlined herein, the onion sites are specific to the Tor Network, which enables user to operate hidden websites, that conceal the true IP address of the computer hosting the website.

address was linked to BTC address bc1qf9vnxeg2pctk9r2mktwd5nt8fqv6u5rthp5uml, hereafter referred to as the **Target CSAM BTC address**, and both addresses were clustered with six (6) other BTC addresses within one (1) BTC wallet.

32. Coinbase referenced the existence of IWF report(s) related to the **Target CSAM BTC address** and **Tor CSAM site 1 BTC address**.

33. On September 13, 2023, I utilized a Tor browser, accessed **Tor CSAM site 1**, and conducted an evidentiary video capture. At this time, I verified this website, entitled "PREMIUM CP," advertised CSAM. I observed one (1) CSAM video, depicting a prepubescent female child, under a section of the website entitled "Sample video" and nine (9) other CSAM videos, depicting prepubescent female children, under a section entitled "SOME SAMPLES OF OUR GALLERY," on the homepage of the website. I watched the "Sample video" revealing an approximately seventeen second video focused on a male touching his erect penis in a masturbatory fashion as he ejaculated into the mouth and face of a prepubescent female child whose upper body is nude. Upon ejaculating into the child's mouth, she begins to gag.

34. **Tor CSAM site 1** identified itself as "a child porn photo and video collection website" existing since 2015 where you could "find over 320,000+ photos and over 70,000+ homemade porn videos of girls and boys from 3 to 16

years old." **Tor CSAM site 1** also contained the text, "To start using our site, you need to buy premium access. To do this, you need to send a unique amount to the bitcoin wallet of our bot." In addition, the site directed potential purchasers to "Deposit 0.0006539 to this wallet BTC: bc1qp9hcrmdpI08ufasnI67q4ef53chmhq38mslwhu", hereafter referred to as **Tor CSAM site 1 BTC address 2**.

35. On September 13, 2023, I conducted database and online queries related to Alec WHITE revealing the following information, in summary:

> Name: Alec Joseph WHITE
> DOB (date of birth): 04/13/1990
> SSN (social security number): XXX-XX-9847
> NC driver's license (DL) number: 000024398976
> Registered vehicle: 2019 Toyota Camry assigned NC/US license plate number B124CP
> Recent potential address: 100 Village Circle Way, Apt 534 Durham, NC 27713

36. On or about September 15, 2023, HSI Raleigh submitted a DHS summons to Coinbase requesting information related to Alec WHITE's account and activity. Coinbase responded and provided the following identity information, in summary:

> Name: Alec WHITE
> Birthdate: 04/13/1990
> SSN (social security number): xxx-xx-9847
> User ID: 5e94b88a25792c1aafb31eb9
> Email address: alecwhite13@icloud.com (deleted)

Phone number: 3363078432 (deleted)
Most recent billing address: 100 Village Circle Way, Apt. 534, Durham, NC 27713
Account creation date: April 13, 2020

Coinbase also provided two (2) photographs depicting the back and front of Alec Joseph WHITE's (DOB: 04/13/1990) NC driver's license (DL), number 000024398976.

37. Coinbase also provided information related to the cryptocurrency transactions from Alec WHITE's account. I reviewed these transactions and identified the following information, in summary, regarding transactions between Alec WHITE's account and the **Target CSAM BTC address**:

1. Timestamp: 8/1/2023 17:50 (5:50:25 PM)
Account Name: BTC Wallet
Type: Send
Status: Complete
Amount: -0.00052924
Currency: BTC
To: bc1qf9vnxeg2pctk9r2mktwd5nt8fqv6u5rthp5uml
Equivalent USD: -15.74
TXHASH:
114af8397fa67877c27362a9cf600e1c26e9d7a5ca7393223d840b59403f2d22

2. Timestamp: 8/1/2023 18:14 (6:14:43 PM)
Account Name: BTC Wallet
Type: Send
Status: Complete
Amount: -0.00032347
Currency: BTC
To: bc1qf9vnxeg2pctk9r2mktwd5nt8fqv6u5rthp5uml
Equivalent USD: -9.66

TXHASH:
621205b582aded627c262995ae70aed195046e076c2f4ce3655733307cbb4892

3. Timestamp: 8/1/2023 21:43 (9:43:36 PM)
Account Name: BTC Wallet
Type: Send
Status: Complete
Amount: -0.00052893
Currency: BTC
To: bc1qf9vnxeg2pctk9r2mktwd5nt8fqv6u5rthp5uml
Equivalent USD: -15.69
TXHASH:
f9a39b5f4a14ee4dc525639f304de0bda79886c9123addcfdfff42f2b89a704d

4. Timestamp: 8/1/2023 22:03 (10:03:40 PM)
Account Name: BTC Wallet
Type: Send
Status: Complete
Amount: -0.00042821
Currency: BTC
To: bc1qf9vnxeg2pctk9r2mktwd5nt8fqv6u5rthp5uml
Equivalent USD: -12.69
TXHASH:
4acf68fd5191509e9d09b4b13f485561bb6bfd3b117cf11df7da5fcd635b30ef

38. Furthermore, I reviewed the events section of the report provided by Coinbase and discovered evidence of VPNs (virtual private networks), Tor, and anonymous proxy usage on Alec WHITE's Coinbase account. I utilized the online geolocation sourcing service maxmind.com to research the IP addresses identified by Coinbase to have accessed Alec WHITE's account revealing periodic usage of VPNs, Tor, and anonymous proxies beginning on 11/24/2021 20:58 (8:58:18 PM) through 8/8/2023 3:02 (3:02:02 AM), which is consistent

with a user attempting to conceal their identity. Within this report, Coinbase also identified location data for some of the IP addresses used to access Alec WHITE's account revealing multiple countries, including the United States, Germany, the Netherlands, and Norway. Additional review of this location data revealed geolocation to different countries on the same date, within minutes of one another, providing further evidence of the usage of VPNs, Tor and/or anonymous proxies to access Alec WHITE's account. Furthermore, within the details portion of the events section on the report, Coinbase documented "tor_user" for Alec WHITE's account on 8/2/2023 at 8:03 (8:03:54 AM).

39. On September 20, 2023, I emailed Coinbase and requested any other documentation they had regarding the **Target CSAM BTC address**. Coinbase responded and provided a screenshot from an open-source intelligence report referencing IWF serial (report) number 3144402 and the IWF's assessment, on August 18, 2023, of an onion URL (website) dedicated to CSAM which provided the **Target CSAM BTC address** for payment purposes.

40. On September 20, 2023, I emailed the IWF and requested copies of any reports they had referencing the **Target CSAM BTC address**. The IWF responded and provided the contents from serial (report) number 3144402. I

reviewed this information revealing the IWF identified assessing a Tor .onion website, which they identified as being dedicated to CSAM, on August 18, 2023. The IWF provided the Tor .onion URL (web address), hereafter referred to as **Tor CSAM site 2**, from the payment page, entitled Teen Porn 24 | Membership, of this website.

41. The IWF identified their assessment revealed the **Target CSAM BTC address**, which they categorized as a commercial CSAM crypto currency address, on the payment page of **Tor CSAM site 2**. The IWF documented they also discovered **Tor CSAM site 2** identified a subscription rate of $15 for 43535 videos with instructions to send 0.00057 of BTC to the **Target CSAM BTC address** on the payment webpage.

42. In addition, the IWF's reporting included the text, "We have assessed the website associated with the above stated report number. The site indicates that it provides paid access to criminal content and offers Cryptocurrency as a suggested payment option" regarding their assessment of **Tor CSAM site 2**.

43. On September 22, 2023, I utilized a Tor browser, accessed **Tor CSAM site 2**, and conducted an evidentiary video capture. I verified this website, entitled "24 Teen Porn 24 – Teen Sex Videos," advertised CSAM. I observed forty-four total images from associated videos on the homepage under

sections entitled, "Hottest Teen Sex Videos Today," "Top Rated Teen XXX Videos" and "New Teen Porn Videos." Forty of the forty-four images are CSAM and show child sexual abuse (CSA) depicting prepubescent and minor aged female and male children, and the other four (4) images depict child erotica. For example, one image depicts an adult male's erect penis partially inserted into the anus of a nude prepubescent aged female child. As a second example, one image depicts a male's erect penis partially inserted into the genitals of what appears to be a partially clothed prepubescent female child near toddler age. Below these forty-four images was the following text:

> Step into the world of teen porn and browse the one and only teenporn24, probably the only site for adults to provide exclusive teen content. Nothing but quality teen sex videos which won't be available for streaming on other pages. Simply connect to this fabulous sex tube and get started. The features are plenty and you will enjoy a smooth navigation. All that thanks to the page's intuitive layout and great options. Either you like them naughty, sensual or wild, the teens on this page will suit even your deepest desires. That's because some are into anal, others are into DP sex and many of them also love taking the jizz on their faces. Feel free to browse teenporn24 and navigate the endless seas of premium teen sex videos available. It's easy and daily updated with new stuff so that you can never get bored. Not to mention the category list which will offer you direct access to all the kinky teen stuff you have been craving for.

44. While conducting the evidentiary video capture, I clicked on a button entitled "SIGN UP" at the bottom of the homepage which led to a

registration page reading, "Membership to TeenPorn24 for a charge of $15 43535 videos" that included areas for the inputting of a username and password. At this time, I entered a fictitious username and password into the webpage and clicked continue which led to another webpage containing the following text, in summary:

> Payment Information
> Waiting for your funds...
> 0.00057 BTC
> UNPAID
> Send the indicated amount to the address below
> 0.00057 BTC
> bc1qp9hcrmdpI08ufasnI67q4ef53chmhq38mslwhu

45. Following the evidentiary video capture, I identified BTC address bc1qp9hcrmdpI08ufasnI67q4ef53chmhq38mslwhu, previously cited within this affidavit as **Tor CSAM site 1 BTC address 2**, was the same BTC address discovered during the evidentiary video capture of **Tor CSAM site 1** on September 13, 2023.

46. On September 25, 2023, I emailed the IWF and requested a copy of the screen capture they took during their documentation of **Tor CSAM site 2**, during their assessment as part of serial (report) number 3144402. The IWF responded and provided the requested screen capture which was dated August 18, 2023. I reviewed the screen capture and visually verified it depicts the membership registration/payment webpage from **Tor CSAM site 2**, as

observed during my evidentiary video capture of the website on September 22, 2023. As observed in the screen capture, **Tor CSAM site 2** included instructions to send 0.00057 of BTC to the **Target CSAM BTC address** as payment. Visual comparison of the IWF screen capture of **Tor CSAM site 2's** membership registration/payment webpage to **Tor CSAM site 2's** membership registration/payment webpage during my evidentiary video capture revealed the only difference appeared to be the BTC addresses provided to purchase additional access to CSAM through the website. As previously cited, the BTC addresses from the IWF screen capture and the evidentiary video capture of **Tor CSAM site 2** have been discovered on Tor .onion CSAM websites.

47. On October 13, 2023, I conducted surveillance at 100 Village Circle Way, Apartment 534, Durham, NC 27713. At approximately 0650 hours, I observed Alec Joseph WHITE's white Toyota Camry, bearing NC license plate number B124CP, parked in a space directly in front of the SUBJECT PREMISES. At approximately, 0720 hours, I observed Alec Joseph WHITE walking from the third floor, down the stairs and to his Camry. I then watched Alec Joseph WHITE enter his Camry and drive away.

48. On October 16, 2023, HSI Raleigh submitted a DHS summons to Spectrum (Charter Communications) requesting subscriber information for

addresses 100 Village Circle Way, Apartment 534, Durham, NC 27713 and 100 Village Circle Way, Apartment 532, Durham, NC 27713. Charter Communications responded and provided the following information, in summary, regarding Apartment 532:

> Customer Name: Alec WHITE
> Email: alecwhite13@icloud.com
> Phone number: (336) 307-8432
> Connection date: 09/07/2023

Charter responded and provided the following information, in summary, regarding Apartment 534:

> Customer Name: Grace Lena
> Email: glena17@ad.unc.edu
> Phone number: (845) 476-2966
> Connection date: 09/10/2023

49. On January 20, 2024, I conducted surveillance at the SUBJECT PREMISES and observed Alec Joseph WHITE arrive in and park his Toyota Camry, bearing NC license plate number B124CP, in front of the 500 building at 100 Village Circle Way, Durham, NC 27713, and the stairs leading to Apartment 532.

50. On March 8, 2024, I conducted law enforcement database queries of the NC Division of Motor Vehicles (DMV) revealing Alec Joseph WHITE had been issued an updated driver's license (DL), number 000024398976, on

February 27, 2024, listing his residential address as 100 Village Circle Way, Apt 532, Durham, NC 27713.

51. In summary, as previously documented within paragraphs 29 through 46 of this Affidavit, Alec WHITE's Coinbase account was utilized, on August 1, 2023, to send BTC to the **Target CSAM BTC address**. On August 18, 2023, the IWF identified the **Target CSAM BTC address** on **Tor CSAM site 2**, which they screen captured. On September 22, 2023, I conducted an evidentiary video capture of **Tor CSAM site 2** and verified it as a website dedicated to CSAM and containing instructions on how to purchase additional access to CSAM. At this time, **Tor CSAM site 2** contained **Tor CSAM site 1 BTC address 2**. On September 25, 2023, the IWF provided their screen capture of the **Target CSAM BTC address** on **Tor CSAM site 2**. I reviewed this screen capture and visually verified it depicts the membership registration/payment webpage from **Tor CSAM site 2**. Visual comparison of the IWF screen capture of **Tor CSAM site 2's** membership registration/payment webpage to **Tor CSAM site 2's** membership registration/payment webpage during my evidentiary video capture revealed the only difference appeared to be the BTC addresses provided to purchase additional access to CSAM through the website.

CHARACTERISTICS COMMON TO INDIVIDUALS WHO PRODUCE, ADVERTISE, TRANSPORT, DISTRIBUTE, RECEIVE, POSSESS, AND/OR ACCESS WITH INTENT TO VIEW CHILD PORNOGRAPHY

52. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know the following are certain characteristics common to individuals who possess, receive and/or distribute child pornography:

a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Such individuals almost always possess and maintain their hard copies of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain their pictures, films, video tapes, photographs, magazines, negatives, correspondence, mailing lists, books, tape recordings and child erotica for many years.

d. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, or in cloud-based online storage, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis.

e. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers

and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.

f. Such individuals also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses (including email addresses), and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

g. Such individuals prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

h. Even if the individual utilizing Alec WHITE's Coinbase account to send BTC to the **Target CSAM BTC address** to purchase and/or attempt to purchase access to **Tor CSAM site 2**, who is believed to be Alec Joseph WHITE, uses a portable device (such as a mobile phone) to access the Internet and child pornography, it is more likely

than not that evidence of this access will be found in his home, the SUBJECT PREMISES, as set forth in Attachment A, and on Alec Joseph WHITE's person, as set forth in Attachment B, and in the SUBJECT VEHICLE, as set forth in Attachment C, including on digital devices other than the portable device (for reasons including the frequency of "backing up" or "synching" mobile phones to computers or other digital devices).

53. Based on the following, I believe the suspected target of this investigation, Alec Joseph WHITE, residing at the SUBJECT PREMISES likely displays characteristics common to individuals who possess, receive, distribute and/or maintain access with intent to view child pornography.

As detailed herein, the target of this investigation, who is believed to be Alec Joseph WHITE, appeared to have accessed **Tor CSAM site 2** and utilized his Coinbase account to send BTC to the **Target CSAM BTC address** to purchase and/or attempt to purchase access to additional CSAM on **Tor CSAM site 2**.

BACKGROUND ON CHILD PORNOGRAPHY, COMPUTERS, AND THE INTERNET

54. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Digital cameras and computers with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as "WiFi" or "Bluetooth." Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos.

c. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Mobile devices such as smartphones and tablet computers may also connect to other computers via wireless connections. Electronic contact can be made to literally millions of computers around the world. Child pornography can therefore be easily, inexpensively and anonymously (through electronic

communications) produced, distributed, and received by anyone with access to a computer or smartphone.

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various types - to include computer hard drives, external hard drives, CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices that are plugged into a port on the computer - can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Some media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also often carried on an individual's person.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide email services and/or electronic

storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as "cloud" storage) from any computer or smartphone with access to the Internet. Such an account can also be accessed in the same way. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer, smartphone, or external media in most cases.

g. A growing phenomenon related to smartphones and other mobile computing devices is the use of mobile applications, also referred to as "apps." Apps consist of software downloaded onto mobile devices that enable users to perform a variety of tasks, such as engaging in online chat, sharing digital files, reading a book, or playing a game, on a mobile device. Individuals commonly use such apps to receive, store, distribute, and advertise child pornography, to interact directly with other like-minded offenders or with potential minor victims, and to access cloud-storage services where child pornography may be stored.

h. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (*i.e.*, by saving an email as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files) or unintentional. Digital information, such as the

traces of the path of an electronic communication, may also be automatically stored in many places (*e.g.*, temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

i. Individuals involved in the receipt, possession, and/or distribution of child pornography very frequently possess multiple devices that contain evidence of their interaction with child pornography and/or sexual interest in minors. In modern American culture, most individuals possess multiple devices that have the ability to connect to the Internet (e.g., tablets, desktop computers, laptop computers, and mobile phones). Many individuals also keep prior versions of their devices (e.g., prior cell phones and prior computers). This is the case because (1) individuals are often reluctant to discard devices that frequently contain significant personal information and (2) current devices may malfunction, and prior versions can often be used until the current device is repaired or replaced.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

55. As described above and in Attachment D, this application seeks permission to search for records that might be found at the SUBJECT PREMISES, on the person of Alec Joseph WHITE, and in the SUBJECT VEHICLE, in whatever form they are found. One form in which the records are likely to be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

56. I submit that if a computer or storage medium is found at the SUBJECT PREMISES, on the person of Alec Joseph WHITE, and in the SUBJECT VEHICLE, there is probable cause to believe those records referenced above will be stored on that computer or storage medium, for at least the following reasons:

a. Deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

b. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years

after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

57. As further described in Attachment D, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described in the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium at the SUBJECT PREMISES, on the person of Alec Joseph WHITE, and in the SUBJECT VEHICLE, at the time of the execution of the warrant because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about

the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. Information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (*e.g.*, registry information, communications, images and movies, transactional information, records of session times and durations, Internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating, or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, computers typically contain information that logs computer user account session times and durations, computer activity associated with user accounts, electronic storage media that

connected with the computer, and the IP addresses through which the computer accessed networks and the Internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (*e.g.*, a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (*e.g.*, Internet searches indicating criminal planning), or consciousness of guilt (*e.g.*, running a "wiping" program to destroy evidence on

the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the

presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to obtain or access child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and, also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of a crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

58. Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained

by corporations, including but not limited to "cloud" storage. I also know that during the search of the premises and/or person it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process that requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software, or operating system that is being searched.

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate

analysis of the equipment and storage devices from which the data will be extracted.

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

59. Additionally, based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of wireless routers, which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be secured (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or unsecured (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime, including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

60. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some, or all of the evidence described in the warrant and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

PROCEDURE FOR UNLOCKING ENCRYPTED DEVICES

61. The search warrant requests authorization to use the biometric unlock features of a device (including phones and computers), as described in Attachment D, based on the following, which I know from my training, experience, and review of publicly available materials:

a. Users may enable a biometric unlock function on some digital devices (including phones and computers). To use this function, a user generally displays a physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a device enabled

with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.

b. In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when a device has been restarted or inactive, has not been unlocked for a certain period of time (often 48 hours or less), or after a certain number of unsuccessful unlock attempts. Thus, the opportunity to use a biometric unlock function even on an enabled device may exist for only a short time. I do not know the passcodes of the devices likely to be found in the search.

Thus, the warrant I am applying for would permit law enforcement personnel to, with respect to any device that appears to have a biometric sensor and falls within the scope of the warrant: (1) depress Alec Joseph WHITE's thumb and/or fingers on the device(s); and (2) hold the device(s) in front of Alec Joseph WHITE's face with his eyes open to activate the facial-, iris-, and/or retina-recognition feature.

CONCLUSION

62. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits, and instrumentalities of these offenses, more fully described in Attachment D, are located at the SUBJECT

PREMISES, described in Attachment A, on the person of Alec Joseph WHITE, described in Attachment B, and in the SUBJECT VEHICLE, described in Attachment C. I respectfully request that this Court issue search warrants for the location(s) and/or person described in Attachment A, B and C, authorizing the seizure and search of the items described in Attachment D.

/S/William Thompson
William Thompson
Special Agent
Homeland Security Investigations

Pursuant to Rule 4.1 of the Federal Rules of Criminal Procedure, the affiant appeared before me via reliable electronic means (telephone), was placed under oath, and attested to the contents of the written affidavit.

04/5/24

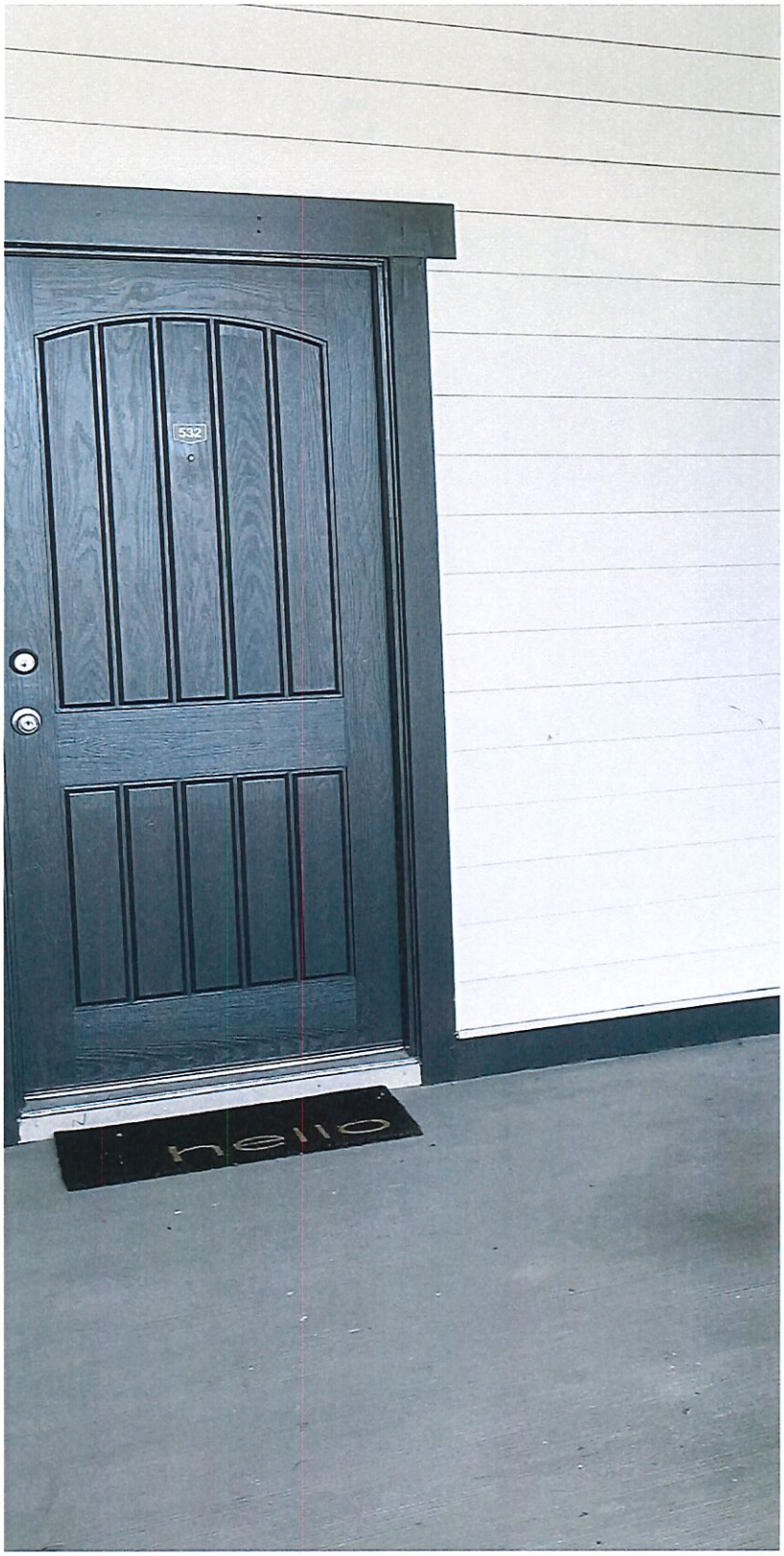
HON. L. PATRICK AULD
UNITED STATES MAGISTRATE JUDGE
MIDDLE DISTRICT OF NORTH CAROLINA

ATTACHMENT A

(Description of Property to be Searched)

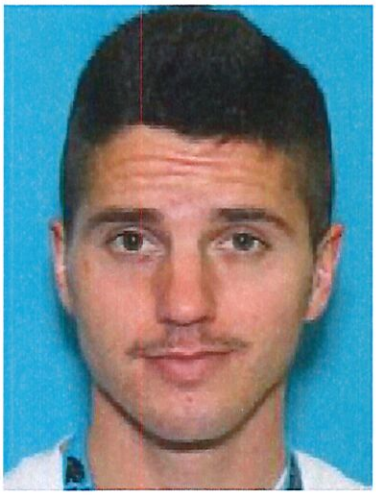
The entire premises located at 100 Village Circle Way, Apartment 532, Durham, North Carolina 27713, (all which constitute the SUBJECT PREMISES. The SUBJECT PREMISES is a single-story, single-family apartment on the third floor of building 500, a multi-unit primarily beige-colored apartment building with dark trim and a shingled roof, inside the Southpoint Village Apartments community. The numerals "500" are posted on the wall of the building near the stairs leading to the SUBJECT PREMISES and the numerals "532" are posted on the front door of the SUBJECT PREMISES. A photo of the front of building 500, including the stairwell leading to the SUBJECT PREMISES, and a photo of the SUBJECT PREMISES' front door are below:


500


532
hello

ATTACHMENT B

(Person to be Searched)



Alec Joseph WHITE (depicted above)

DOB: 04/13/1990

ATTACHMENT C

(Description of Vehicle to be Searched)

The vehicle, and digital devices contained therein, described as follows: a white 2019 Toyota Camry assigned NC license plate number B124CP and registered to Alec Joseph WHITE at the SUBJECT PREMISES.

ATTACHMENT D

(Items to be Seized)

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use, or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, Sections 2252A(a)(2)(A) and 2252A(a)(5)(B):

1. Computers or storage media that could be used as a means to commit the violations described above, and on which the things described in this warrant could be stored, which may then be searched for the items set out below.
2. Routers, modems, and network equipment used to connect computers to the Internet.
3. Child pornography and child erotica.
4. Records and information relating to violations of the statutes described above in the form of:
    a. Records and information referencing or revealing the occupancy or ownership of the SUBJECT PREMISES, 100 Village Circle Way, Apartment 532, Durham, North Carolina 27713;

b. Records and information referencing or revealing the use or ownership of the Coinbase account with User ID 5e94b88a25792c1aafb31eb9;

c. Records and information referencing or revealing the use of Tor to access the Tor .onion website entitled 24 Teen Porn 24 – Teen Sex Videos;

d. Records and information referencing or revealing the distribution, advertising, or possession of child pornography, to include the identity of the individuals involved and location of occurrence;

e. Records and information referencing or revealing a sexual interest in children or the sexual exploitation of children, to include the identity of the individuals involved and location of occurrence;

f. Records and information referencing or revealing communication or interaction of an illicit sexual nature with minors, to include the identity of the individuals involved and location of occurrence;

g. Records and information referencing or revealing participation in groups or the use of services that are known to be used to facilitate the distribution and/or storage of child pornography;

h. Records and information referencing or revealing the use of remote computing services such as email accounts or cloud storage.

5. For any computer or storage medium whose seizure is otherwise authorized by this warrant (hereinafter, "COMPUTER"):

   a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, deleted, viewed, or otherwise interacted with;

   b. evidence of how and when the COMPUTER was used to create, edit, delete, view, or otherwise interact with or engage in the things described in this warrant;

   c. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

   d. evidence of the Internet Protocol addresses used by the COMPUTER;

   e. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

   f. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

   g. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of

malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

h. evidence of the lack of such malicious software;

i. evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;

6. During the course of the search, photographs of the location to be searched may be taken to record the condition thereof and/or the location of items therein.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, smartphones, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.

During the execution of the search of the SUBJECT PREMISES as described in Attachment A, Alec Joseph WHITE's person as described in Attachment B, and the SUBJECT VEHICLE described in Attachment C, law enforcement personnel are also specifically authorized to compel Alec Joseph WHITE if present at the time of the execution of the warrant, to provide biometric features, including pressing fingers (including thumbs) against and/or putting a face before the sensor, or any other security feature requiring biometric recognition, of:

a. any of the DEVICES found at the SUBJECT PREMISES, on Alec Joseph WHITE's person, and in the SUBJECT VEHICLE, and

b. where the DEVICES are limited to which are capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities of the offense(s) as described in the search warrant affidavit and warrant attachments, for the

purpose of attempting to unlock the DEVICES' security features in order to search the contents as authorized by this warrant, but only if Alec Joseph WHITE is present at the time of the execution and the process is carried out with dispatch in the immediate vicinity of the SUBJECT PREMISES, on Alec Jospeh WHITE, or in the SUBJECT VEHICLE.

This warrant does not authorize law enforcement personnel to compel any other individuals found at the SUBJECT PREMISES to provide biometric features, as described in the preceding paragraph, to access or otherwise unlock any DEVICE. Further, this warrant does not authorize law enforcement personnel to request that any individuals present at the SUBJECT PREMISES state or otherwise provide the password or any other means that may be used to unlock or access the DEVICES, including by identifying the specific biometric characteristics (including unique finger(s) or other physical features) that may be used to unlock or access the DEVICES.

PRECAUTIONARY INSTRUCTIONS TO PRESERVE POTENTIAL PRIVILEGES

If, during the execution of this warrant, the government discovers materials that are potentially attorney-client privileged or subject to the work product doctrine ("protected materials"), the Prosecution Team will

discontinue its review until the potentially protected materials have been segregated from other evidence obtained under this warrant. Prior to any further review of the identified potentially protected materials, the Government will notify the Court of the need to establish a court-approved process for review and filtering of the potentially protected materials.